

Bounds on Network Codes for the Homogeneous Weight

Eimear Byrne

*School of Mathematics and Statistics,
University College Dublin, Ireland*

Abstract

We give upper bounds on the size of a code whose fundamental parameters are determined by a directed acyclic graph that has a single source node, a set of sink nodes \mathcal{T} and n edges. A code associated with this digraph is a collection $\mathcal{C} := \{\mathcal{C}_t \subset \mathcal{A}^{n_t} : t \in \mathcal{T}\}$ where n_t is the number of edges incident with sink t and \mathcal{A} is an R - R bimodule for a finite ring R . For each $t \in \mathcal{T}$, the ambient space \mathcal{A}^{n_t} of \mathcal{C}_t is $\mathcal{F}_t(\mathcal{A}^n)$ for a left R -epimorphism \mathcal{F}_t . Then \mathcal{A}^{n_t} is equipped with a weight function w_t induced by a weight function w on \mathcal{A}^n via $w_t(\mathcal{F}_t(x)) = \min\{w(y) : x - y \in \ker \mathcal{F}_t\}$. We use the classical Plotkin and Elias bounds to derive upper bounds on the quantity $\min\{|\mathcal{C}_t| : t \in \mathcal{T}\}$ as we range over all such codes $\mathcal{C} := \{\mathcal{C}_t \subset \mathcal{A}^{n_t} : t \in \mathcal{T}\}$.

Keywords: network code, network error-correction, coherent networks, Plotkin bound, Elias bound, finite Frobenius ring, homogeneous weight

1. Introduction

Coding in data communication networks has been shown to offer many advantages in terms of data rate, error correction and security. Many coding models have been considered for a variety of networks. Error-correction for coherent networks has been considered in [10, 14, 15, 16, 19]. For so called non-coherent networks, where the network topology is unknown, subspace codes have been shown to offer good solutions for error correction and have been widely studied.

We consider the set-up for coherent network coding introduced in [17]. The network $\mathcal{N} = (V, E)$ is a directed acyclic graph with nodes/vertices V and edge set E of order n . We assume that \mathcal{N} has a single source node s incident with some m outgoing edges and has several sinks labelled by elements of a set \mathcal{T} . A message of m packets is transmitted from the source node to be received at each sink in \mathcal{T} . For each sink $t \in \mathcal{T}$, let E_t denote the set of edges incident with t and let $|E_t| = n_t$. We furthermore assume that $n_t \geq m$ for each t and indeed that there are at least m edge disjoint paths connecting s to t . We will adopt a linear coding scheme, which means, as usual, that at each node in the network, linear combinations of packets on its incoming edges are transmitted along its outgoing edges. In our context, the underlying alphabet is a finite

Email address: ebyrne@ucd.ie (Eimear Byrne)

bimodule and the codes are equipped with a distance function induced by the *homogeneous weight*. This very general model includes the case where the alphabet is a finite fields and the induced metric comes from the Hamming weight and so extends the coding model described in [17]. Furthermore, we develop upper bounds on codes associated with fixed network based on the Plotkin and Elias bounds. These results are new both for the classical case of a finite fields and in the more general case of a finite Frobenius bimodule².

In Section 2 we give a formal description of a code for a fixed network digraph. In Section 3 we outline preliminaries on the homogeneous weight for code modules defined over finite Frobenius bimodule. In Section 4 we present an upper bound on the size of a network code based on Plotkin's bound and in Section 5 we give an Elias-like bound. In Section 6 we give asymptotic versions of these bounds.

2. Codes Associated with a Network

Let R be a finite ring with unity and let \mathcal{A} be a finite R - R bimodule. The set of messages for \mathcal{N} is a subset \mathcal{M}_0 of \mathcal{A}^m . Each message $x_0 \in \mathcal{M}_0$ corresponds to a unique network word $x = [x_0, 0] \in \mathcal{M} := \{[u, 0] : u \in \mathcal{M}_0\} \subset \mathcal{A}^n$, canonically embedding \mathcal{A}^m into \mathcal{A}^n . The network itself may be identified with \mathcal{A}^n , where each i -th coordinate projection from \mathcal{A}^n onto \mathcal{A} corresponds to the i -th edge of the network, under some ordering.

A word $z \in \mathcal{A}^n$ is transmitted along the network by an invertible transfer map

$$\mathcal{F} : \mathcal{A}^n \longrightarrow \mathcal{A}^n : z \mapsto (f_1(z), \dots, f_n(z)),$$

for some R -linearly independent maps $f_j \in \text{Hom}_R(\mathcal{A}^n, \mathcal{A})$. If $x \in \mathcal{A}^n$ is transmitted from the source node s and some edges of the network are corrupted by errors in the form of an error word $e \in \mathcal{A}^n$ then the network transmission is given by $y = \mathcal{F}(x + e)$. In other words, it is assumed that errors propagate through the network.

In the context of [10] (which is an error-free model) \mathcal{F} is represented by an invertible transfer matrix $F \in R^{n \times n}$ with respect to some fixed basis. The network coding model described in [15, 16, 19] results from the case $R = \mathcal{A} = GF(q)$. The approach in [14] corresponds to the case $R = GF(q)$ and $\mathcal{A} = GF(q)^r$.

For each $t \in \mathcal{T}$, let $\Pi_t : \mathcal{A}^n \longrightarrow \mathcal{A}^{n_t} : z \mapsto (z_j)_{j \in E_t}$ be the projection onto the coordinates indexed by the edges incident with t and define a map

$$\mathcal{F}_t := \Pi_t \circ \mathcal{F} : \mathcal{A}^n \longrightarrow \mathcal{A}^{n_t}.$$

In the multicast setting, for each $t \in \mathcal{T}$, we require that $\mathcal{F}_t : \mathcal{M} \longrightarrow \mathcal{A}^{n_t}$ be an injection, in order that each sink t can decode the transmitted word to the same unique message in \mathcal{M} .

²The results given here were presented at the International Workshop in Coding and Cryptography, Bergen in 2013 [1]. The finite field case has been considered independently in [18].

Definition 1. Let \mathcal{N} be a network with transfer map $\mathcal{F} \in \text{Aut}_R(\mathcal{A}^n)$. The network code for node t of $(\mathcal{N}, \mathcal{F})$ is the set

$$\mathcal{C}_t := \{\mathcal{F}_t(x) \in \mathcal{A}^{n_t} : x \in \mathcal{M}\} \subset \mathcal{A}^{n_t}.$$

The network code of $(\mathcal{N}, \mathcal{F})$ is the collection $\mathcal{C} := \{\mathcal{C}_t : t \in \mathcal{T}\}$.

Note that neither \mathcal{M} nor any \mathcal{C}_t need be R -linear; the linearity of \mathcal{C} refers only to linearity of the transfer map \mathcal{F} .

The received word at node t is given by $y_t = \mathcal{F}_t(x + e)$. We denote by \mathcal{K}_t the kernel of the map \mathcal{F}_t in \mathcal{A}^n so that $\mathcal{C}_t = \mathcal{F}_t(\mathcal{M}) \subset \mathcal{A}^{n_t} \cong \mathcal{A}^n / \mathcal{K}_t$. Observe that if $e \in \mathcal{K}_t$ then $y_t = \mathcal{F}_t(x + e) = \mathcal{F}_t(x)$ is received as if no errors have occurred. If $m = n_t$, the kernel \mathcal{K}_t is trivial and the decoder will not detect any errors.

A weight function w on \mathcal{A}^n induces a weight w_t on \mathcal{A}^{n_t} as follows:

$$w_t(u) := w(x + \mathcal{K}_t) = \min\{w(z) : \mathcal{F}_t(z) = u\},$$

for some x in the preimage of u under \mathcal{F}_t . If w determines a distance function d on \mathcal{A}^n by $d(x, y) := w(x - y)$, then $d_t(u, v) := w_t(u - v)$ is also a distance function on \mathcal{A}^{n_t} .

Given the received word y_t , the decoder at node t decides that $c = \mathcal{F}_t(x)$ has been transmitted if $d_t(y_t, c) < d_t(y_t, c')$ for all $c' \in \mathcal{C}_t$.

Example 1. Let $R = \mathcal{A} = GF(q)$ and let w denote the usual Hamming weight on $GF(q)^n$. Let \mathcal{N} be a network and let \mathcal{C}_t be a network code for \mathcal{N} at one of its sink nodes t . \mathcal{F}_t has a representation as an $n \times n_t$ matrix F_t with respect to a chosen basis. Then $w_t(u) = \min\{w(z) : zF_t = u\} = w(x + \mathcal{K}_t)$ counts the minimum number of linearly independent rows of F_t required to obtain a representation of $u = xF_t$. If $x \in \mathcal{M}$ is transmitted and y is received at t , the decoder will decode to $y - eF_t \in \mathcal{C}_t$ for some error $e \in GF(q)^n$ of least Hamming weight satisfying $y = (x + e)F_t$. In other words the decoder assumes that the least number of edges resulting in a non-trivial contribution to the computation of y have been affected by noise during transmission.

We denote by d_t the minimum distance of \mathcal{C}_t with respect to d_t . We write ℓ_t to denote the size of the support of \mathcal{K}_t . For each $t \in \mathcal{T}$, we write \mathcal{M}_t to denote the preimage of \mathcal{C}_t in \mathcal{A}^{n_t} and we let $s_t := |\text{supp}(\mathcal{M}_t)|$. Clearly $|\mathcal{A}|^{s_t} \geq |\mathcal{M}_t| = |\mathcal{K}_t||\mathcal{C}_t| = |\mathcal{A}|^{n-n_t}|\mathcal{C}_t|$ and $|\mathcal{C}_t| \leq |\mathcal{A}|^{s_t-n+n_t}$.

We say that \mathcal{C} is an $(n, \{(n_t, \ell_t, |\mathcal{C}_t|, d_t) : t \in \mathcal{T}\})$ network code. We define $s(\mathcal{C}) := \min\{|\mathcal{C}_t| : t \in \mathcal{T}\}$, which we call the size of \mathcal{C} , and seek upper bounds on this number, which is the effective maximum possible size of the message space \mathcal{M} .

Definition 2. We denote by $A(n, \{(n_t, \ell_t, d_t) : t \in \mathcal{T}\})$ the maximum size $s(\mathcal{C})$ of any $(n, \{(n_t, \ell_t, |\mathcal{C}_t|, d_t) : t \in \mathcal{T}\})$ network code \mathcal{C} .

3. Modules and Homogeneous Weights

The homogeneous weight was first introduced on the ring \mathbb{Z}_m in [3]. Generalizations of this weight function have appeared in [4, 5, 8]. For coding theoretic purposes, these are often best defined on a *Frobenius bimodule*.

We define a weight function, or weight on an R -module M to be a map $w : M \rightarrow \mathbb{R}$ such that $w(0) = 0$. The homogeneity conditions in [4] are given by the following.

Definition 3. A weight function w on a left R -module M is called (left) homogeneous if

H1 If $Rx = Ry$ then $w(x) = w(y)$ for all $x, y \in M$.

H2 There exists a real number γ such that

$$\sum_{y \in Rx} w(y) = \gamma |Rx| \quad \forall 0 \neq x \in M. \quad (1)$$

Right homogeneous weights are defined similarly. In [8] condition H2 is given as:

H2' There exists a real number γ such that

$$\sum_{x \in V} w(x) = \gamma |V| \quad \forall 0 \neq V < {}_R M. \quad (2)$$

In fact, if ${}_R M$ is a left *Frobenius module*, in particular if its socle is cyclic, then H2 implies H2'. Moreover, a homogeneous weight function exists on any finite module ${}_R M$ and is unique up to choice of average weight γ [8].

Example 2. For the case $R = M = GF(q)$, the Hamming weight is homogeneous with average weight $\gamma = \frac{q-1}{q}$. For the case $R = M = \mathbb{Z}_4$, the Lee weight is homogeneous with average weight $\gamma = 1$.

Example 3. Let $R = M = GF(q)^{2 \times 2}$. Then it is straightforward to check that the weight function w on M defined by

$$w(x) = \begin{cases} \frac{q^3 - q^2 - q}{q^3 - q^2 - q + 1} & \text{if } \text{rank}_{GF(q)}(x) = 2, \\ \frac{q^2}{q^2 - 1} & \text{if } \text{rank}_{GF(q)}(x) = 1, \\ 0 & \text{if } x = 0, \end{cases}$$

is homogeneous with average value $\gamma = 1$.

For the case $R = GF(q)$, $M = GF(q)^{2 \times 2}$, only the Hamming weight, for $\gamma = \frac{q-1}{q}$, is homogeneous.

We extend w to a weight function on \mathcal{A}^n in the obvious way:

$$w : \mathcal{A}^n \longrightarrow \mathbb{R} : w(c_1, \dots, c_n) \mapsto \sum_{i=1}^n w(c_i).$$

In [4], the authors show that every finite unital ring R has a quasi-Frobenius bimodule, which is unique up to right and left R -isomorphism if its socle is cyclic both as a left and right R -module. Such a module is then called a Frobenius bimodule.

Let $\mathcal{A} := \text{Hom}_{\mathbb{Z}}(\mathcal{A}, \mathbb{C}^\times)$, the group of characters of the additive group of \mathcal{A} . $\hat{\mathcal{A}}$ is an R - R bimodule according to the relations

$${}^r \chi(x) = \overline{\chi(rx)}, \quad \chi^r(x) = \chi(xr)$$

for all $r \in R, x \in \mathcal{A}$ and $\chi \in \hat{\mathcal{A}}$. A character $\chi \in \hat{\mathcal{A}}$ is called (left) generating if given any $\phi \in \hat{R}$ there is some $r \in R$ satisfying $\phi = {}^r \chi$. This is equivalent to the property that $\ker \chi$ contains no left R -submodule of \mathcal{A} .

Definition 4. The bimodule ${}_R\mathcal{A}_R$ is a Frobenius bimodule if

$${}_R\mathcal{A} \cong {}_R\hat{R} \text{ and } \mathcal{A}_R \cong \hat{R}_R.$$

By duality, if ${}_R\mathcal{A}_R$ is Frobenius then ${}_R\hat{\mathcal{A}} \cong {}_R R$ and $\hat{\mathcal{A}}_R \cong R_R$. In particular, if ${}_R\mathcal{A}_R$ is a Frobenius bimodule then $\hat{\mathcal{A}}$ is generated by a character χ both as a left and as a right R -module.

The existence of such a generating character $\chi \in \hat{\mathcal{A}}$ gives the following characterisation of the homogeneous weight on a Frobenius bimodule (cf [7]). The proof is straightforward.

Lemma 1. Let ${}_R\mathcal{A}_R$ be a Frobenius bimodule with generating character χ . Then the weight function

$$w : \mathcal{A} \longrightarrow \mathbb{R} : a \mapsto \gamma \left(1 - \frac{1}{|R^\times|} \sum_{u \in R^\times} \chi(xu) \right)$$

is homogeneous.

For a positive integer k , word $z \in \mathcal{A}^k$ and set $X \subset \{1, \dots, k\}$ we define $\pi_X(z) := (z_i)_{i \notin X} \in \mathcal{A}^{k-|X|}$. Given an R -submodule $M < \mathcal{A}^k$, we write $\text{supp}(M)$ to denote the set $\{i : \pi_i(c) \neq 0 \text{ some } c \in M\}$, where $\hat{i} := \{1, \dots, k\} \setminus \{i\}$ for each i .

Using the character-theoretic description of the homogeneous weight given above, the following result can be shown, with the proof proceeding almost exactly as in [2, Lemma 1].

Lemma 2. Let ${}_R\mathcal{A}_R$ be a Frobenius bimodule with homogenous weight function $w : \mathcal{A} \longrightarrow \mathbb{R}$. Let M be an R -submodule of \mathcal{A}^n and let $x \in \mathcal{A}^n$. Then

$$\sum_{c \in M} w(x+c) = \gamma |M| |\text{supp}(M)| + |M| w(\pi_{\text{supp}(M)}(x)).$$

Unless stated otherwise, for the remainder we assume that \mathcal{A} is a Frobenius bimodule and that for each linear map $\mathcal{F}_t : \mathcal{A}^n \longrightarrow \mathcal{A}^{n_t}$ the weight function w_t is induced by the homogeneous weight w on \mathcal{A} , extended to a weight on \mathcal{A}^n .

4. A Plotkin-Like Bound

We seek an upper bound on $|\mathcal{C}_t|$ for each $(n_t, \ell_t, |\mathcal{C}_t|, d_t)$ code \mathcal{C}_t . Following the usual argument for the classical Plotkin bound, we obtain lower and upper bounds on $\sum_{c, c' \in \mathcal{C}_t} d_t(c, c')$. Proposition 2.1 of [6] gives a Plotkin bound for codes over finite Frobenius rings with respect to the homogeneous weight, which has the trivial extension:

Lemma 3. Let $C \subset \mathcal{A}^n$ have minimum homogeneous distance $d(C)$. Then

$$|C|(|C| - 1)d(C) \leq \sum_{x, y \in C} w(x - y) \leq \gamma n |C|^2.$$

Theorem 4. Let $\mathcal{C}_t \subset \mathcal{A}^{n_t}$ be the $(n_t, |\mathcal{C}_t|, d_t)$ network code for node t . If $d_t > \gamma s_t$ then

$$|\mathcal{C}_t| \leq \frac{d_t - \gamma \ell_t}{d_t - \gamma s_t}.$$

PROOF. We give an estimate of the sum of the distances between ordered pairs of distinct codewords of \mathcal{C}_t :

$$\begin{aligned} |\mathcal{C}_t|(|\mathcal{C}_t| - 1)d_t &\leq \sum_{\mathcal{F}_t(x), \mathcal{F}_t(y) \in \mathcal{C}_t} w_t(\mathcal{F}_t(x) - \mathcal{F}_t(y)), \\ &= \sum_{\mathcal{F}_t(x), \mathcal{F}_t(y) \in \mathcal{C}_t} w(x - y + \mathcal{K}_t), \\ &\leq \sum_{\mathcal{F}_t(x), \mathcal{F}_t(y) \in \mathcal{C}_t} \frac{1}{|\mathcal{K}_t|} \sum_{k \in \mathcal{K}_t} w(x - y + k), \\ &= \frac{1}{|\mathcal{K}_t|^2} \sum_{\substack{x, y \in \mathcal{M}_t : \\ x - y \notin \mathcal{K}_t}} w(x - y), \\ &= \frac{1}{|\mathcal{K}_t|^2} \left(\sum_{x, y \in \mathcal{M}_t} w(x - y) - \sum_{\substack{x, y \in \mathcal{M}_t : \\ x - y \in \mathcal{K}_t}} w(x - y) \right), \\ &= \frac{1}{|\mathcal{K}_t|^2} \left(\sum_{x, y \in \mathcal{M}_t} w(x - y) - |\mathcal{C}_t| |\mathcal{K}_t| \sum_{z \in \mathcal{K}_t} w(z) \right), \\ &\leq |\mathcal{C}_t|^2 s_t \gamma - |\mathcal{C}_t| \ell_t \gamma, \end{aligned}$$

from Lemmas 2 and 3. Now rearrange to obtain

$$|\mathcal{C}_t| \leq \frac{d_t - \gamma \ell_t}{d_t - \gamma s_t},$$

as long as $d_t > \gamma s_t$.

We remark that if $\ell_t = s_t$ then the inequality $(|\mathcal{C}_t| - 1)d_t \leq |\mathcal{C}_t| s_t \gamma - \ell_t \gamma$ implies that $d_t \leq s_t \gamma$. If \mathcal{K}_t is trivial then $\ell_t = 0$ and Theorem 4 is the classical Plotkin bound [6, Theorem 2.2].

Corollary 5. Let $d = \min\{d_t : t \in \mathcal{T}\} > \gamma n$ and let $\ell = \min\{\ell_t : t \in \mathcal{T}\}$. Then

$$A(n, \{(n_t, \ell_t, d_t) : t \in \mathcal{T}\}) \leq \min \left\{ \frac{d_t - \gamma \ell_t}{d_t - \gamma n} : t \in \mathcal{T} \right\} \leq \frac{d - \gamma \ell}{d - \gamma n}.$$

PROOF.

$$\frac{d_t - \gamma \ell_t}{d_t - \gamma s_t} \leq \frac{d_t - \gamma \ell_t}{d_t - \gamma n} \leq \frac{d_t - \gamma \ell}{d_t - \gamma n} \leq \frac{d - \gamma \ell}{d - \gamma n}.$$

Observe that the upper bound in Corollary 5 depends on n, ℓ_t and d_t , but not on n_t .

Corollary 6. *Let $d = \min\{d_t : t \in \mathcal{T}\} > \gamma n$. Then*

$$A(n, \{(n_t, \ell_t, d_t) : t \in \mathcal{T}\}) \leq \min \left\{ 1 + \frac{\gamma n_t}{d - \gamma s_t} : t \in \mathcal{T} \right\} \leq \min \left\{ 1 + \frac{\gamma n_t}{d - \gamma n} : t \in \mathcal{T} \right\}.$$

PROOF. \mathcal{K}_t can be embedded in \mathcal{A}^{ℓ_t} , so that $|\mathcal{K}_t| = |\mathcal{A}|^{n-n_t} \leq |\mathcal{A}|^{\ell_t}$. Then $n \geq s_t \geq \ell_t \geq n - n_t \geq s_t - n_t$, so the result follows.

5. An Elias-Like Bound

The results of this section rely on [6], applied to \mathcal{C}_t , giving an upper bound on $|\mathcal{C}_t|$ for the case $d_t < \gamma n$. We recall the following well-known lemma (see, for example [11, Lemma 5.2.9]).

Lemma 7. *Let $A, B \subset \mathcal{A}^N$. Then there exists $x \in \mathcal{A}^N$ such that*

$$|B| \leq \frac{|(x+A) \cap B| |\mathcal{A}|^N}{|A|}.$$

For each nonnegative real number r we define

$$B_t^{\text{av}}(r) := \{z \in \mathcal{A}^{n_t} : \frac{1}{|\mathcal{K}_t|} \sum_{\mathcal{F}_t(x)=z} w(x) \leq r\}.$$

It is easy to deduce from this lemma that

$$|\mathcal{C}_t| \leq \frac{|B_t^{\text{av}}(r) \cap \mathcal{C}_t| |\mathcal{A}|^{n_t}}{|B_t^{\text{av}}(r)|}. \quad (3)$$

To simplify notation, for each $t \in \mathcal{T}$ and vector $x \in \mathcal{A}^n$, we write

$$\pi_t(x) := (x_i)_{i \notin \text{supp } \mathcal{K}_t} \in \mathcal{A}^{n-\ell_t} \text{ and } \pi'_t(x) := (x_i)_{i \in \text{supp } \mathcal{K}_t} \in \mathcal{A}^{\ell_t}.$$

Note that if $\mathcal{F}_t(x) = \mathcal{F}_t(y)$ for some $x, y \in \mathcal{A}^n$ then $\pi_t(x) = \pi_t(y)$. We will use this elementary fact throughout.

Corollary 8. *Let $r \geq \ell_t \gamma$. Then*

$$B_t^{\text{av}}(r) = \{\mathcal{F}_t(x) \in \mathcal{A}^{n_t} : w(\pi_t(x)) \leq r - \ell_t \gamma\}.$$

PROOF. Let $z \in \mathcal{A}^{n_t}$. Applying Lemma 2, $z \in B_t^{\text{av}}(r)$ if and only if

$$r \geq \frac{1}{|\mathcal{K}_t|} \sum_{\mathcal{F}_t(x)=z} w(x) = \gamma \ell_t + w(\pi_t(x)).$$

Corollary 9. *Let $r \geq \gamma \ell_t$. Then*

$$|B_t^{\text{av}}(r)| = |B^{n-\ell_t}(r - \gamma \ell_t)| |\mathcal{A}|^{\ell_t - n + n_t}.$$

PROOF. Let $x \in \mathcal{A}^n$. From Corollary 8, $\mathcal{F}_t(x) \in B_t^{\text{av}}(r)$ if and only if $\pi_t(x) \in B^{n-\ell_t}(r - \gamma\ell_t)$. Let $\mathcal{K}_t' := \{\pi_t'(z) : z \in \mathcal{K}_t\} \subset \mathcal{A}^{\ell_t}$. Clearly $|\mathcal{K}_t'| = |\mathcal{K}_t|$, so there are exactly $|\mathcal{A}|^{\ell_t - n + n_t}$ distinct cosets of \mathcal{K}_t' in \mathcal{A}^{ℓ_t} . Then for each $u \in B^{n-\ell_t}(r - \gamma\ell_t)$, there are exactly $|\mathcal{A}|^{\ell_t - n + n_t}$ distinct elements $\mathcal{F}_t(x) \in \mathcal{A}^{n_t}$ satisfying $\pi_t(x) = u$.

The following is now immediate.

Theorem 10. *Let $r - \gamma\ell_t > 0$ for each $t \in \mathcal{T}$. Then*

$$A(n, \{(n_t, \ell_t, d_t) : t \in \mathcal{T}\}) \leq \min \left\{ \frac{|B_t^{\text{av}}(r) \cap \mathcal{C}_t| |\mathcal{A}|^{n-\ell_t}}{|B^{n-\ell_t}(r - \gamma\ell_t)|} : t \in \mathcal{T} \right\}. \quad (4)$$

We now obtain an upper bound on the size of $B_t(r) := B_t^{\text{av}}(r) \cap \mathcal{C}_t$. Clearly, $B_t(r)$ has minimum distance $d_t(B_t(r)) \geq d_t$.

For each $t \in \mathcal{T}$, let $\{x_1, \dots, x_{|B_t(r)|}\}$ be a set of distinct coset representatives of \mathcal{K}_t in $\mathcal{F}_t^{-1}(B_t(r))$. We denote by B_t^π the multiset of words in $\mathcal{A}^{n-\ell_t}$ constructed as

$$B_t^\pi := \{\pi_t(x_1), \dots, \pi_t(x_{|B_t(r)|})\},$$

where $|B_t^\pi(r)| = |B_t(r)|$.

Theorem 11. *Let $r \geq \gamma\ell_t$. Then*

$$|B_t(r)|(|B_t(r)| - 1)(d_t - \gamma\ell_t) \leq \sum_{u, v \in B_t^\pi} w(u - v).$$

PROOF. Using Lemma 2, we obtain

$$\begin{aligned} |B_t(r)|(|B_t(r)| - 1)d_t &\leq \sum_{\mathcal{F}_t(x), \mathcal{F}_t(y) \in B_t(r)} w_t(\mathcal{F}_t(x) - \mathcal{F}_t(y)) \\ &\leq |B_t(r)|(|B_t(r)| - 1)\gamma\ell_t + \sum_{\mathcal{F}_t(x), \mathcal{F}_t(y) \in B_t(r)} w(\pi_t(x - y)), \\ &= |B_t(r)|(|B_t(r)| - 1)\gamma\ell_t + \sum_{u, v \in B_t^\pi} w(u - v). \end{aligned}$$

Lemma 12. *Let $r \geq \gamma\ell_t$. Then $d(B_t^\pi(r)) \geq d_t - \gamma\ell_t$.*

PROOF. As before, let $\mathcal{K}_t' := \{\pi_t'(z) : z \in \mathcal{K}_t\} \subset \mathcal{A}^{\ell_t}$. Let $u, v \in B_t^\pi(r)$. Let $x, y \in \mathcal{F}_t^{-1}(B_t(r))$ satisfy $\pi_t(x) = u, \pi_t(y) = v$, and

$$\begin{aligned} d_t \leq d_t(\mathcal{F}_t(x), \mathcal{F}_t(y)) &= w(x - y + \mathcal{K}_t) \\ &= w(\pi_t'(x) - \pi_t'(y) + \mathcal{K}_t') + w(\pi_t(x) - \pi_t(y)) \\ &\leq \gamma\ell_t + w(u - v). \end{aligned}$$

In particular $d(B_t^\pi(r)) \geq d_t - \gamma\ell_t$.

We have the following result, given in the proof of [6, Corollary 3.3].

Lemma 13. *Let $s \leq \gamma N$ and let $W \subset \mathcal{A}^N$. If $w(v) \leq s$ for every $v \in W$ then*

$$\sum_{u,v \in W} w(u-v) \leq 2|W|^2 s - |W|^2 \frac{s^2}{\gamma N}.$$

Observing that the above result is valid for a multiset of words W , and then substituting $N = n - \ell_t$, $s = r - \gamma \ell_t$, $W = B_t^\pi(r)$, and $d(B_t^\pi(r)) \geq d_t - \gamma \ell_t$ immediately gives:

Corollary 14. *Let $r \leq \gamma n$ and let $n > \ell_t$. Then*

$$|B_t(r)|(|B_t(r)| - 1)(d_t - \gamma \ell_t) \leq 2|B_t(r)|^2(r - \gamma \ell_t) - |B_t(r)|^2 \frac{(r - \gamma \ell_t)^2}{\gamma(n - \ell_t)}.$$

Moreover, if $r \leq \gamma n - \sqrt{\gamma(n - \gamma \ell_t)(\gamma n - d_t)}$ then

$$|B_t(r)| \leq f(r, n, \ell_t, d_t) := \frac{\gamma(d_t - \gamma \ell_t)(n - \ell_t)}{(r - \gamma n)^2 - \gamma(\gamma n - d_t)(n - \gamma \ell_t)}.$$

Theorem 15. *Let $d_t \leq \gamma n$ and let $\gamma \ell_t \leq r \leq \gamma n - \sqrt{\gamma(\gamma n - d_t)(n - \gamma \ell_t)}$. Then*

$$|\mathcal{C}_t| \leq \frac{f(r, n, \ell_t, d_t) |\mathcal{A}|^{n - \ell_t}}{|B^{n - \ell_t}(r - \gamma \ell_t)|}.$$

In particular if the above hypothesis holds for each $t \in \mathcal{T}$, then

$$A(n, \{(n_t, \ell_t, d_t) : t \in \mathcal{T}\}) \leq \min \left\{ \frac{f(r, n, \ell_t, d_t) |\mathcal{A}|^{n - \ell_t}}{|B^{n - \ell_t}(r - \gamma \ell_t)|} : t \in \mathcal{T} \right\}.$$

6. Asymptotic Bounds

Asymptotic versions of these bounds are expressed by finding upper bounds on:

$$\alpha_{\mathcal{A}}(\{(v_t, \lambda_t, \delta_t) : t \in \mathcal{T}\}) := \limsup_{n \rightarrow \infty} n^{-1} \log_{|\mathcal{A}|} (A(n, \{(v_t n, \lambda_t n, \delta_t n) : t \in \mathcal{T}\})).$$

As in the classical Hamming case, we will require an asymptotic expression for the size of the homogeneous sphere $B^N(\delta N) \subset \mathcal{A}^N$. This was essentially answered first in [12] and in a slightly different form (which we use here) in [6, Theorem 4.1] as follows:

Lemma 16. *For all $\delta \in [0, \gamma]$ there holds:*

$$\lim_{N \rightarrow \infty} \sup N^{-1} \log_{|\mathcal{A}|} |B^N(\delta N)| = \min \left\{ \log_{|\mathcal{A}|} \left(\sum_{a \in \mathcal{A}} Z^{w(a) - \delta} \right) : Z \in (0, 1] \right\}.$$

Definition 5. Let $\delta \geq 0$. We define the function

$$H_{\mathcal{A}}(\delta) := \min \left\{ \log_{|\mathcal{A}|} \left(\sum_{a \in \mathcal{A}} Z^{w(a) - \delta} \right) : Z \in (0, 1] \right\}.$$

6.1. An Asymptotic Plotkin Bound

Theorem 17.

$$\alpha_{\mathcal{A}}(\{(v_t, \lambda_t, \delta_t) : t \in \mathcal{T}\}) \leq \begin{cases} 0 & \text{if } \delta > \gamma \\ 1 - \frac{\delta}{\gamma} & \text{if } \delta \leq \gamma \end{cases}$$

where $\delta = \min\{\delta_t : t \in \mathcal{T}\}$

PROOF. If $\delta > \gamma$ then from Corollary 5 it is clear that $\alpha_{\mathcal{A}}(\{(v_t, \lambda_t, \delta_t) : t \in \mathcal{T}\}) = 0$. Now suppose that $\delta \leq \gamma$. Let $\mathcal{C} = \{\mathcal{C}_t : t \in \mathcal{T}\}$ be an optimal $(n, \{(n_t, \ell_t, |\mathcal{C}_t|, d_t) : t \in \mathcal{T}\})$ network code and choose t such that $\delta_t = \delta$. Let $d = \delta n$. Then $\gamma \ell_t < \gamma s_t < d \leq \gamma n$. Choose n' to be the greatest integer satisfying $\gamma n' \leq d - 1$. Then $n - n' > 0$ and $n' > \ell_t$ by our choice of n' . Consider the words of $\mathcal{M}_t \subset \mathcal{A}^n$. By a standard coding theory argument we can take $s_t - n'$ successive shortenings of \mathcal{M}_t on its coordinates in $\text{supp}(\mathcal{M}_t) \setminus \text{supp}(\mathcal{K}_t)$ to arrive at a code in \mathcal{A}^n of order at least $\frac{|\mathcal{M}_t|}{|\mathcal{A}|^{s_t - n'}} \geq \frac{|\mathcal{M}_t|}{|\mathcal{A}|^{n - n'}}$. Then puncture the code on these coordinates, as well as any coordinate not in $\text{supp}(\mathcal{M}_t)$, to obtain a code $M' \subset \mathcal{A}^{n'}$ of the same order. The corresponding code K' obtained by puncturing \mathcal{K}_t on the same coordinates satisfies $|K'| = |\mathcal{K}_t|$ and so the set of words of M' is a union of at $\frac{|\mathcal{C}_t|}{|\mathcal{A}|^{n - n'}}$ distinct cosets of K' in $\mathcal{A}^{n'}$. This yields a code C' satisfying $d(C') = d' \geq d > \gamma n'$. Again apply Corollary 5 to get

$$\frac{s(\mathcal{C})}{|\mathcal{A}|^{n - n'}} \leq \frac{|\mathcal{C}_t|}{|\mathcal{A}|^{n - n'}} \leq |C'| \leq \frac{d - \gamma \ell_t}{d - \gamma n'} \leq d - \gamma \ell_t = \delta n - \gamma \lambda_t n.$$

Then

$$\begin{aligned} \alpha_{\mathcal{A}}(\{(v_t, \lambda_t, \delta_t) : t \in \mathcal{T}\}) &\leq \limsup_{n \rightarrow \infty} n^{-1} \log_{|\mathcal{A}|} |\mathcal{A}|^{n - n'} (\delta n - \gamma \lambda_t n) \\ &\leq 1 - \limsup_{n \rightarrow \infty} \frac{n'}{n} + \frac{\log_{|\mathcal{A}|} (\delta n - \gamma \lambda_t n)}{n} \\ &= 1 - \frac{\delta}{\gamma}. \end{aligned}$$

6.2. An Asymptotic Elias Bound

Theorem 18. Let \mathcal{T} be a non-empty set and let $\rho > 0$. For each $t \in \mathcal{T}$ let $v_t, \lambda_t, \delta_t \in (0, 1)$ satisfy $\delta_t \leq \gamma$, $\gamma \lambda_t \leq \rho \leq \gamma - \sqrt{\gamma(\gamma - \delta_t)(1 - \gamma \lambda_t)}$. For each positive integer n define

$$h_n(u, v) := \frac{f(\rho, 1, u, v)|\mathcal{A}|^{n(1-u)}}{|B^{n(1-u)}(n(\rho - \gamma u))|},$$

$(\lambda, \delta) := \text{argmin}\{h_n(\lambda_t, \delta_t) : t \in \mathcal{T}\}$ and $\xi := \frac{\rho - \gamma \lambda}{1 - \lambda}$. Then

$$\limsup_{n \rightarrow \infty} n^{-1} \log_{|\mathcal{A}|} (A(n, \{(v_t n, \lambda_t n, \delta_t n) : t \in \mathcal{T}\})) \leq 1 - \lambda - H_{\mathcal{A}}(\xi).$$

In particular,

$$\alpha_{\mathcal{A}}(\{v_t, \delta_t, \lambda_t : t \in \mathcal{T}\}) \leq 1 - \lambda - H_{\mathcal{A}}\left(\gamma - \sqrt{\frac{\gamma(\gamma - \delta)(1 - \gamma\lambda)}{1 - \lambda}}\right).$$

PROOF. From Theorem 15 we have $A(n, \{(v_t n, \lambda_t n, \delta_t n) : t \in \mathcal{T}\}) \leq h_n(\lambda, \delta)$. Then

$$\begin{aligned} & \lim_{n \rightarrow \infty} n^{-1} \log_{|\mathcal{A}|} (A(n, \{(v_t n, \lambda_t n, \delta_t n) : t \in \mathcal{T}\})) \\ & \leq \lim_{n \rightarrow \infty} n^{-1} \log_{|\mathcal{A}|} (h_n(\lambda, \delta)) \\ & = \lim_{n \rightarrow \infty} n^{-1} \log_{|\mathcal{A}|} \left(\frac{f(\rho, 1, \lambda, \delta)|_{\mathcal{A}} n^{(1-\lambda)}}{|B^{n(1-\lambda)}(n(\rho - \gamma\lambda))|} \right) \\ & = 1 - \lambda - \lim_{n \rightarrow \infty} n^{-1} \log_{|\mathcal{A}|} (|B^{n(1-\lambda)}(\xi(n(1-\lambda)))|) \\ & = (1 - \lambda) - H_{\mathcal{A}}(\xi) \end{aligned}$$

Since this holds true for any choice of ρ , by continuity of $H_{\mathcal{A}}$, the final inequality holds.

As $\lambda \rightarrow 0$, the upper bound on $\alpha_{\mathcal{A}}(\{v_t, \delta_t, \lambda_t : t \in \mathcal{T}\})$ given above becomes the asymptotic Elias bound of [6].

- [1] E. Byrne, “On Bounds for Network Codes,” International Workshop in Coding and Cryptography, Bergen, April 15-19, 2013, preprint available at <http://www.selmner.uib.no/WCC2013/PreProceedings.pdf>, pp. 476–576.
- [2] E. Byrne, M. Greferath, A. Kohnert, V. Skachek, “New Bounds for Codes Over Finite Frobenius Rings”, Designs, Codes and Cryptography, **57**, pp. 169–179, 2010.
- [3] I. Constantinescu and W. Heise, “A Metric for Codes Over Residue Class Rings of Integers”, Problems Inform. Transmission, **33**, pp. 147–153, 1997.
- [4] M. Greferath, A. Nechaev, and R. Wisbauer, “Finite Quasi-Frobenius Modules and Linear Codes”, J. Algebra and Applications, **3**, no. 3, pp. 247–272, 2004.
- [5] M. Greferath and S. E. Schmidt, “Finite-Ring Combinatorics and MacWilliams Equivalence Theorem”, J. Combin. Theory Ser. A, **92**, pp. 17–28, 2000.
- [6] M. Greferath and M. E. O’Sullivan, “On Bounds for Codes Over Frobenius Rings Under Homogeneous Weights”, Discrete Mathematics, **289**, pp. 11–24, 2004.
- [7] T. Honold, “A Characterization of Finite Frobenius Rings”, Arch. Math. (Basel), **76**, pp. 406–415, 2001.
- [8] T. Honold and A. A. Nechaev, “Weighted Modules and Representations of Codes”, Problems Inform. Transmission, **35**, pp. 205–223, 1999.

- [9] W. C. Huffman and V. Pless, *Fundamentals of Error Correcting Codes*, Cambridge, 2003.
- [10] R. Koetter and M. Medard, “An Algebraic Approach to Network Coding”, IEEE/ACM Transactions on Networking, **11**, Issue 5, pp. 782–795, 2003.
- [11] J. H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, 1999.
- [12] H. Loeliger, “An Upper Bound on the Volume of Discrete Spheres”, IEEE Transactions on Information Theory, **40**, No. 6, pp. 2071–2073, 1994.
- [13] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.
- [14] D. Silva, F. Kschichang and R. Kötter, “Communication over Finite-Field Matrix Channels”, IEEE Trans. Inf. Theory, **56**, pp. 1296–1305, 2010.
- [15] S. Yang, C. K. Ngai and R. Yeung, “Construction of Linear Network Codes that Achieve a Refined Singleton Bound”, IEEE International Symposium on Information Theory, pp. 1576–1580, June 2007.
- [16] S. Yang and R. Yeung, “Refined Coding Bounds for Network Error Correction”, IEEE Information Theory Workshop on Information Theory for Wireless Networks, pp. 1–5, July 2007.
- [17] S. Yang, R. Yeung and C. K. Ngai, “Refined Coding Bounds and Code Constructions for Coherent Network Error Correction”, IEEE Transactions on Information Theory, Vol. 57, No. 3, pp. 1409–1423, 2011 .
- [18] Q. Wang and S. Jaggi, “End-to-End Error-Correcting Codes on Networks with Worst-Case Symbol Errors,” arXiv:1510.03060, 2015.
- [19] Z. Zhang, “Linear Network Error Correction Codes in Packet Networks”, IEEE Transactions on Information Theory, **54**, Issue 1, pp. 209–218, 2008.